

CLAIMS

What is claimed is:

1 1. An apparatus comprising:
2 a processor having a normal execution mode and a secure execution
3 environment to create a secure execution environment; and
4 a secure virtual machine monitor (SVMM) to implement the secure
5 execution mode in which a plurality of separate virtual machines are created that
6 operate simultaneously and separately from one another including at least a first virtual
7 machine to implement trusted guest software in a protected memory area and a second
8 virtual machine to implement a non-trusted guest operating system (OS) in a non-
9 protected' memory area;
10 wherein responsive to a command to tear down the secure execution
11 environment, the SVMM causes the processor to exit out of the secure execution mode,
12 tears down the secure execution environment, and instructs the non-trusted guest OS to
13 resume control in the normal execution mode.

1 2. The apparatus of claim 1, further comprising a virtual machine control
2 structure (VCMS) to store guest state information related to the non-trusted guest
3 operating system (OS) for use in restoring the non-trusted guest OS in the normal
4 execution mode.

1 3. The apparatus of claim 2, wherein the virtual machine control structure
2 (VCMS) stores a guest OS entry point field to point to a command used for instructing
3 the non-trusted guest OS to resume control at a virtual address and a host entry point
4 field to point to a command to instruct the processor to exit out of a virtual machine
5 execution mode.

1 4. The apparatus of claim 1, further comprising, the SVMM scrubbing the
2 protected memory associated with the trusted guest software when the secure execution
3 environment is torn down.

1 5. The apparatus of claim 4, further comprising, the SVMM causing the
2 processor to exit out of a virtual machine extension mode before exiting out of the
3 secure execution mode when the secure execution environment is torn down.

1 6. The apparatus of claim 1, wherein the non-trusted guest operating
2 system (OS) issues the command to tear down the secure execution environment.

1 7. The apparatus of claim 1, wherein the secure virtual machine monitor
2 (SVMM) issues the command to tear down the secure execution environment.

1 8. The apparatus of claim 7, wherein the secure virtual machine monitor
2 (SVMM) issues the command to tear down the secure execution environment due to a
3 detected security breach.

1 9. A method comprising:
2 providing a normal execution mode in a processor and a secure
3 execution mode in a processor; and
4 creating a secure execution environment in which a plurality of separate
5 virtual machines operate simultaneously and separately from one another including at
6 least a first virtual machine to implement trusted guest software in a protected memory
7 area and a second virtual machine to implement a non-trusted guest operating system
8 (OS) in a non-protected memory area;
9 wherein responsive to a command to tear down the secure execution
10 environment, exiting out of the secure execution mode, tearing down the secure
11 execution environment, and instructing the non-trusted guest OS to resume control in
12 the normal execution mode.

1 10. The method of claim 9, further comprising storing guest state
2 information related to the non-trusted guest operating system (OS) for use in restoring
3 the non-trusted guest OS in the normal execution mode.

1 11. The method of claim 10, further comprising:
2 storing a guest OS entry point field to point to a command used for
3 instructing the guest OS to resume control at a virtual address; and
4 storing a host entry point field to point to a command to instruct the
5 processor to exit out of a virtual machine execution mode.

1 12. The method of claim 9, further comprising scrubbing the protected
2 memory associated with the trusted guest software when the secure execution
3 environment is torn down.

1 13. The method of claim 12, further comprising causing the processor to exit
2 out of a virtual machine extension mode before exiting out of the secure execution
3 mode when the secure execution environment is torn down.

1 14. The method of claim 9, wherein the non-trusted guest operating system
2 (OS) issues the command to tear down the secure execution environment.

1 15. The method of claim 9, further comprising issuing the command to tear
2 down the secure execution environment due to a detected security breach.

1 16. A machine-readable medium having stored thereon instructions, which
2 when executed by a machine, cause the machine to perform the following operations
3 comprising:

4 providing a normal execution mode in a processor and a secure
5 execution mode in a processor; and

6 creating a secure execution environment in which a plurality of separate
7 virtual machines that operate simultaneously and separately from one another including
8 at least a first virtual machine to implement trusted guest software in a protected
9 memory area and a second virtual machine to implement a non-trusted guest operating
10 system (OS) in a non-protected memory area;

11 wherein responsive to a command to tear down the secure execution
12 environment, exiting out of the secure execution mode, tearing down the secure
13 execution environment, and instructing the non-trusted guest OS to resume control in
14 the normal execution mode.

1 17. The machine-readable medium of claim 16, wherein the instructions
2 cause the machine to perform further operations comprising storing guest state
3 information related to the non-trusted guest operating system (OS) for use in restoring
4 the non-trusted guest OS in the normal execution mode.

1 18. The machine-readable medium of claim 17, wherein the instructions
2 cause the machine to perform further operations comprising:

3 storing a guest OS entry point field to point to a command used for
4 instructing the guest OS to resume control at a virtual address; and

5 storing a host entry point field to point to a command to instruct the
6 processor to exit out of a virtual machine execution mode.

1 19. The machine-readable medium of claim 16, wherein the instructions
2 cause the machine to perform further operations comprising scrubbing the protected
3 memory associated with the trusted guest software when the secure execution
4 environment is torn down.

1 20. The machine-readable medium of claim 19, wherein the instructions
2 cause the machine to perform further operations comprising causing the processor to
3 exit out of a virtual machine extension mode before exiting out of the secure execution
4 mode when the secure execution environment is torn down.

1 21. The machine-readable medium of claim 16, wherein the non-trusted
2 guest operating system (OS) issues the command to tear down the secure execution
3 environment.

1 22. The machine-readable medium of claim 16, wherein the instructions
2 cause the machine to perform further operations comprising issuing the command to
3 tear down the secure execution environment due to a detected security breach.

1 23. A system comprising:

2 a processor including virtual machine extension (VMX)
3 instruction support, the processor further having a normal execution
4 mode and a secure execution mode to create a secure execution
5 environment;

6 a memory including a protected memory area and a non-
7 protected memory area; and

8 a secure virtual machine monitor (SVMM) to implement the
9 secure execution environment in which a plurality of separate virtual
10 machines are created that operate simultaneously and separately from
11 one another including at least a first virtual machine to implement
12 trusted guest software in the protected memory area and a second virtual
13 machine to implement a non-trusted guest operating system (OS) in the
14 non-protected memory area;

15 wherein responsive to a command to tear down the secure
16 execution environment, the SVMM causes the processor to exit out of
17 the secure execution mode, tears down the secure execution
18 environment, and instructs the non-trusted guest OS to resume control in
19 the normal execution mode.

1 24. The system of claim 23, further comprising a virtual machine control
2 structure (VCMS) to store guest state information related to the non-trusted guest
3 operating system (OS) for use in restoring the non-trusted guest OS in the normal
4 execution mode.

1 25. The system of claim 24, wherein the virtual machine control structure
2 (VCMS) stores a guest OS entry point field to point to a command used for instructing
3 the non-trusted guest OS to resume control at a virtual address and a host entry point
4 field to point to a command to instruct the processor to exit out of a virtual machine
5 execution mode.

1 26. The system of claim 23, further comprising, the SVMM scrubbing the
2 protected memory associated with the trusted guest software when the secure execution
3 environment is torn down.

1 27. The system of claim 26, further comprising, the SVMM causing the
2 processor to exit out of a virtual machine extension mode before exiting out of secure
3 execution mode when the secure execution environment is torn down.

1 28. The system of claim 23, wherein the non-trusted guest operating system
2 (OS) issues the command to tear down the secure execution environment.

1 29. The system of claim 23, wherein the secure virtual machine monitor
2 (SVMM) issues the command to tear down the secure execution environment.

1 30. The system of claim 29, wherein the secure virtual machine monitor
2 (SVMM) issues the command to tear down the secure execution environment due to a
3 detected security breach.